Ninth European Annual Conference on
HUMAN DECISION MAKING AND MANUAL CONTROL
Varese, Italy, September 10-12, 1990

PRINCIPLES OF PROCEDURAL SUPPORT IN MAN-MACHINE SYSTEMS

George R.S. Weir
Scottish HCI Centre, George House, North Hanover Street, Glasgow G1 2AD, UK

Erik Hollnagel
CRI A/S, P. O. Box 173, DK-3460 Birkerød, Denmark

1. INTRODUCTION

In process control environments operators are often required to work with complex interface systems. When manual intervention is required the operator needs to identify system states and respond with appropriate remedial or preventative actions. In many cases this may take place under serious time constraints where the complexity in the system interface and the degree of control automation can compound the operator's difficulty by increasing the cognitive demands in the problem solving situation (Bainbridge, 1987; Woods, 1990).

Conventionally, support for manual control (intervention) is available in the form of hard-copy compendiums of standard and emergency operating procedures, put together before the commissioning of each individual plant. Such manuals assist by detailing the pre-conditions, conditions and means for effecting specific changes in the process state. The two main variants are event based procedures and symptom based procedure, cf. Hollnagel et al., 1990. In event based procedures the point of entry is defined by the particular event (accident) type; the operator is therefore required to diagnose the cause of the problem before he can enter and execute the appropriate procedure. In symptom based procedures the actions are specified on the basis of specific indications of the system status. Operators have resort to these manuals as guidance on 'proper' responses to anticipated plant states. Although valuable and widely used, such assistance is limited by a number of factors:

- Procedure manuals provided in a hard-copy form. This clearly limits the convenience with which operators can access the required information. The need physically to manoeuvre large tomes within close proximity to control desks may generate its own problems. In many cases the more frequently used procedures have therefore been provided on separate cards or in booklets, which make them easier to use. A classical example is the checklist used in aviation (Degani & Wiener, 1990).

- Procedures are fixed and inflexible in the degree and form of information they provide. This is mainly due to the dependence on the hard-copy form. A major

step forward in operator convenience lies in making procedural information readily available (on-line) in a manner which is both flexible in mode of expression and sensitive to the context of the current process state. This requires the use of information processing systems (computers), and major improvements have been made over the last decade, particularly in areas where other considerations forbade the use of voluminous hard-copy procedures (e.g. Rouse & Rouse, 1980).

- Procedures address "standard" situations and responses. This limitation is not removed by simply changing the format or the mode of presentation, but requires a completely different approach to procedure specification. A facility that is able to address procedural needs in less familiar contexts will clearly provide substantial benefits for operators.

The present paper describes strategies for operator support which focus upon flexible procedural assistance. This is based upon the use of knowledge-based modules within an intelligent interface for process control.

2. VARIETIES OF PROCEDURAL SUPPORT

De Keyser (1986) characterises four different situations based upon two variable factors: the level of constraint upon the operator (including situation complexity and temporal pressure), and operator response (varying in degree of adaptation to the situation). These four situations are connected with typical system states, as shown in Figure 1.

Insert Figure 1 about here

- In **normal operation** the fluctuation of plant parameters remains within acceptable (manageable) limits. Operators maintain control "by the play of anticipation and the optimization of variables." Here the objective of operator support is "to develop and to integrate to the maximum the operating images, in a way compatible with the economic and safety objective." Procedures are needed to bring the plant from one state to another (e.g. from hot stand-by to full power), but are usually neither required nor provided for balance-of-plant, etc.

- In **subnormal situations** the operators respond to process vagaries by strategies directed principally toward maintenance of plant safety. For this type of situation the objective of operator assistance is "to release him from the temporal constraint and to direct him to the tasks at which he excels."

- In **abnormal situations** the maintenance of safety ceases to be feasible and operators adopt damage limitation strategies. "Operator control tends to become disorganized and closed loop blow-by-blow strategies replace open loop ones." Here the objective of system aid is to contain the operator's panic, shield him from temporal pressure and relieve him of responsibility "by framing and guiding his action."

- Finally, in **"drifting" situations** the plant states moves gradually toward an abnormal state, without the operator being fully aware. There is a clear difference between the actual and the perceived system state. "He repeats unsuccessfully inoperative behaviours, without modifying them, and consults the same information sources without looking for others." The importance is to jog

the operator from a possibly fixated view of the process situation, ideally, forcing the operator to re-evaluate the situation and provide means for readily checking his assumptions.

The significance of these four situations is that they allow us to characterise the form in which operators may benefit from system support, in particular procedural support.

Essentially, a procedure consists of one or more actions (operations) which, in combination, take the agent further toward a desired objective. Taking an example from a communication network domain, we have a procedure for handling a situation in which a communication line or its outserver has gone down. This procedure consists of several steps, which may in themselves be sub-procedures. Thus, the operator must check the line, to determine whether the line or outserver is at fault, then proceed either with a repair server or repair line response. Although the precise detail of this example is not important, it serves to illustrate the sequential stepwise nature of operator procedures. Put most simply, a procedure is a way to do something: the active means whereby a goal may be approached or accomplished. For the case in point, the sequence of operator actions determines whether a line or outserver is at fault, and takes remedial action accordingly.

With this initial understanding, "procedural support" may be assumed to describe any assistance which enhances the operator's capabilities to act procedurally (toward a recognised goal). The analysis by De Keyser, however, made it clear that different types of situations require different types of support and procedures. In some cases support is needed for the straightforward achivement of a goal. In other cases support is needed to reestablish the operator's comprehension of the situation. In both cases procedural support may do the job, but it will be different types of procedures. Above all, the procedural support must be flexible and adaptive, able to take the operator's needs as well as the system state into account.

In what follows, we describe the GRADIENT approach to intelligent operator support, with emphasis upon the needs and scope for procedural assistance.

3. THE GRADIENT APPROACH

The primary objective of the GRADIENT project is to develop a knowledge-based support and interface for operators in control of dynamic processes. This is achieved by an architecture of specialised modules which not only provides on-request information and advice to operators, but also functions as a monitor of the operator and the process. Control of interaction between operators and the GRADIENT system is handled by a knowledge-based dialogue system which drives a graphical interface to the user. A clear principle in the design of the GRADIENT architecture is to meet the demands of operator support through specialisation of system modules. This paper describes the specific performance of two GRADIENT modules in the provision of procedural support.

The support needed by an operator can be described in relation to the temporal development of an event. This produces the following categories:

- **Alarm** or annunciation. The system state must be brought to the attention of the operator.

- **Analysis**. The system state must be identified and the possible lines of action must be specified.
- **Advice**. The alternatives for action must be evaluated.
- **Accomplishment** and approval. The chosen line of action must be executed and the execution must be monitored.
- **Acknowledgement**. Finally, the results of the chosen line of action must be checked to see whether the intended goal state was reached.

The architecture of GRADIENT (shown in Figure 2), provides for a separation of functions within the system which can be related to the above mentioned categories.

- **Alarm**. Process failure detection and indication is achieved through the expert system module QRES.
- **Analysis**. The analysis is supported by a module for state-based diagnosis (CAUSES) and a module for synthesis of operating procedures (PSES).
- **Advice**. The main support for advice is given by a module for consequence prediction (IMPACT).
- **Accomplishment**. The actual execution of the procedure is monitored through an operator response evaluation system (RESQ). The execution may be guided by the dialogue system (DIS).
- **Acknowledgement**. The presentation of information, for this as well as for the other functions, is achieved through a presentation system (PRES) together with a graphical expert system (GES), able to dynamically hone the organisation of graphical display for PRES.

The overall job of handling the operator input and output is addressed by the presentation system (PRES), while dialogue control and content are derived from a dedicated dialogue system (DIS).

Insert Figure 2 about here

The rest of the paper will describe the combined roles of the GRADIENT dialogue system (DIS) and the response evaluation system (RESQ) in the support of operator monitoring and procedure execution, in particular the complementary roles of RESQ and DIS. This serves both to clarify the available scope for operator support and to underline the advantages of GRADIENT's policy of functional separation.

3.1 The Dialogue System (DIS)

The architecture of DIS contains several components which combine to produce the concurrent knowledge-based dialogue facility required in GRADIENT (illustrated in Figure 3)

Insert Figure 3 about here

- The **Inter-Module Communication Handler** has a generic functionality which is also found in other GRADIENT modules. Primarily, its role is to handle the sequencing of input and output between the Dialogue System and other GRADIENT modules.

- **Dialogue Assistants** serve as controllers for instances of dialogue support directed at the operator, or for handling interaction with other GRADIENT modules. These programs effect all their actions through the Dialogue Knowledge Base. Events, which initiate Dialogue Assistants, are also directed through this knowledge base. Dialogue Assistants consist of networks which represent the features of interaction required for particular dialogue tasks. Such tasks will relate to operator objectives for action on the process (cf. Alty & Weir, 1987).

  A special Dialogue Assistant, the **General Purpose Assistant** (GPA), acts as a monitor for other Dialogue Assistants and the RESQ sub-system. The principal role of the GPA is to act as a clearing house for operator actions relayed from the Presentation System. In normal operation, individual Dialogue Assistants will pass through states where they expect to receive acknowledgements of relevant operator actions. Thus, at any time, several Dialogue Assistants will be "listening" for one or other of a small range of possible operator responses. Rather than relay such information directly from the Presentation System to specific Dialogue Assistants, all operator input is monitored by the GPA, which is kept advised of current operator action "interests" held by active Dialogue Assistants. The GPA then signals receipt of the operator action to the interested Dialogue Assistant(s). Should more than one Dialogue Assistant be awaiting the same operator action, this will be appreciated by the GPA, which is in a position to advise all interested parties of any relevant events.

- The **Dialogue Knowledge Base** serves both as a repository of knowledge derived from other GRADIENT modules and provides a distribution point both for this knowledge and for the actions of the Dialogue Assistants.

3.2 Response Evaluation System (RESQ)

The principal role of RESQ is to provide a monitoring and alarm facility which responds to operator actions. This is achieved through the following module structure (illustrated in Figure 4):

Insert Figure 4 about here

- The **Plan Recogniser** processes input from the operator, creates an entry in an action log, and produces a plan graph representing this action. The Plan Recogniser controls the matching of this graph to graphs which represent currently incomplete plans. When all matches for this action are found, the action's set of possible explanations (a structure containing all possible interpretations of the current action in light of previous actions) are passed to the Plan Evaluator. The Plan Recogniser uses the Plan Library to identify which plans the operator's action may be part of. If no path from the action to a high level goal is found, then the action must be erroneous. In this case, the action is passed to the Error Handler.

- The **Plan Evaluator** uses meta-plan rules and the current system status to narrow down and order likely interpretations of the action in question. Meta-plans are stored in sets with the value of the results obtained from these heuristic sets being dynamically determined according to the system status. Thereby, different heuristics may be used for different phases of plant operation. Information from the blackboard may further reduce the number of action interpretations. When multiple interpretations of the operators actions are equally likely, the Plan Evaluator halts and waits for further actions to disambiguate these interpretations.

- The **Error Handler** assesses the severity of the error and determines whether or not to inform the operator or demand operator intervention to correct the error. In addition, the Error Handler uses a knowledge-base of common human error syndromes to attempt to diagnose the error (Hollnagel, 1990). This knowledge-base is based on error phenotypes and includes such common mistakes as forgetting a step in a plan, reversing the order of two steps, and substituting an incorrect action for the correct one. Using this diagnosis of the error RESQ can not only warn the operator of the error but also explain why the error occurred. Where the determination of a remedy for the error does not require deep domain knowledge, the Error Handler will present this remedy to the operator through the Dialogue System.

- The **Plan Library** stores all operator activities in the terms of plans. A plan is defined to consist of a goal and a set of actions with constraints which, when met, achieve that goal. A complex plan may consist of a number of sub-goals as well as actions which may be optional or replaceable. Actions may have time, fact, and equality constraints. The knowledge in the Plan Library is provided in advance by the system designer using design knowledge or extensive knowledge elicitation. All modules in RESQ may access the Plan Library.

- The **Blackboard** contains RESQ's current best guess of what the operator is doing. Specifically, the Blackboard stores the name of the current plan, it's goal, the actions completed so far in this plan and the next expected steps. This information is used to refine further the interpretation as more actions are taken into account, and may be accessed by other modules of the GRADIENT system. Most results on the blackboard are determined by the plan evaluator but other sources may contribute knowledge opportunistically as well. For instance, if the operator requests procedural support from the Support Expert System to achieve a particular goal then SES sends this information to RESQ. Upon determination of the significance of the operator's action(s), as nearly as possible, the Blackboard is updated with the new plan information. If the action completes a high level plan, the actions which contributed towards this plan are considered explained. This explanation is placed in the action log and these actions are no longer considered in further matching.

As in other GRADIENT modules, external communication with RESQ is handled by an Inter-Module Communication Handler.

4. PLANS IN DIS AND RESQ

Clearly, the interpretation of operator plans plays a major role in the functionality of both DIS and RESQ.

RESQ's concern is exclusively with "control plans". This is the term given to any ordered sequence of operator actions aimed at some control objective on the process or control system. Such plans consist in large part of actions which modify the state of the process or of the control equipment. Additionally, they include actions wherein the operator "prepares" for such modification, e.g. by making component selections on his display panel, performing system checks, etc. These aspects of interaction will be used by RESQ to focus its interpretation of the operator's likely plan.

DIS is not exclusively concerned with such control plans. The operator may invoke assistance from the Dialogue System if he has need of a specific information service (e.g., to access another GRADIENT facility). In handling this request, DIS will not relate in any way to plans for operating on the process. On the other hand, the operator may request dialogue support for performing some control or test procedure. In this case, DIS provides assistance directly tied to relevant control plans.

If the operator has not invoked dialogue support for his system interaction, then DIS will not be involved in his interaction, save that the GPA will serve as a relay for RESQ. Under dialogue support, DIS replaces the need for RESQ to follow every step of the possible operator control plan. In such a case, DIS follows the interaction, possibly leading the operator, until he performs some action which directly affects the process or control system. At this point, the relevant action will be signified to RESQ. Where necessary, DIS provides indication of the relevant steps by which this action was reached. In this way, DIS employs subsets of control plans in order to support operators, and incidentally, complements RESQ in its task of following the operator.

The nature of plans and their different representations play a crucial part in the provision of RESQ and DIS support for the operator. Primarily, DIS will operate upon segments of control plans, i.e. each control plan will be represented as a set of sub-sets of the plan as held in RESQ. In DIS, such plans will include additional steps which represent the range of relevant information services available to the operator at each point in the plan ("enriched dialogue"). In this sense, DIS may also maintain plans which are dialogue specific and serve as additional support for assistance with control procedures. Thus, we can appreciate four levels of plan representation:

- as objects in the Plan Library;
- as a sequence of essential actions on the control level (control plans);
- as an enriched sequence of actions on the dialogue level (enriched dialogue); and
- as dialogue sub-plans (dialogue excursions).

Plans as objects and as sequences of control actions are held by RESQ, while the enriched plan sequences (control plans with dialogue supplements) and the non-control dialogue sub-plans are held by DIS.

5. DIS AND RESQ IN OPERATION

Consider a scenario in the data network where a line or server has gone down and the operator is required to take appropriate response. Notification of the line-or-server-down failure will be passed to the operator from QRES, via DIS and PRES. Thereupon, the dialogue system offers assistance in handling the failure situation. This help takes

the form of several options. Dialogue offers a menu from which the operator may select one of the following:

- o information on recent failures and related incidents for the affected node, node's lines and server;
- o a paged account of the normal procedure for handling a line or server down
- o stepping through the recovery procedure without dialogue following the operator's actions
- o being lead through the procedure, ensuring that each step is accomplished in turn.

The first of these options provides a limited information service and involves no details of the appropriate recovery procedure. Information can be specific to the actual node or line which has the failure, or the operator can choose to view data from other parts of the network. This is effectively a dialogue excursion.

The paged account option is also an information service but specific to the required operating procedure. This allows for "gross" access to procedure information by simply displaying a full textual description of the recommended operator response. A facility which displays the procedure as a decision tree or flow chart is a further possibility at this level.

In the third option only action monitoring is provided. Consequently, no attention is paid by DIS to the operator's control actions. It is expected that he will perform the required part of the procedure as each step is presented by dialogue, but no check is made by the active Dialogue Assistant, and no filtering of operator actions is effected by the GPA. Thus, RESQ receives no support from dialogue in this mode.

With the final option, the operator requests full procedural support from dialogue. Here he is "talked" through each of the sub-procedures in turn, i.e., the structure of the procedure is made explicit and organised in stages to reflect the order required for operation. Active Dialogue Assistants will track operator actions as he performs the sub-procedures, select-node, select-line, etc., and the GPA will relay these actions directly to dialogue, away from RESQ. As key points in the procedure are reached (i.e., modifications are made to the control system), these actions are passed to RESQ, which is thus able to follow the progress of the operator without tracking his every action.

6. CONCLUSIONS

The modular design of the GRADIENT system affords several varieties of operator support. In this paper, we have detailed the operation of two specific GRADIENT modules, DIS and RESQ, and the parts that they play in two aspects of operator assistance. We have seen that, while the operations of DIS and RESQ each depend upon plan representations of operator actions, this implies no redundancy in system performance. Rather, the functionalities of DIS and RESQ are dovetailed to provide a blend of operator monitoring and dialogue support for control procedures.

The forms of support afforded by these two modules is clearly diverse. Whereas DIS offers procedural support, RESQ provides operator monitoring. When combined, DIS procedural support filters non-control actions from RESQ (via the GPA), leaving RESQ

to handle the critical operator actions on the process. Without active dialogue support, RESQ is obliged to track all components of operator procedures, including actions which do not directly impinge upon the process, but which otherwise initiate or differentiate control procedures. The result is a high degree of flexibility in operator interaction as well as greater sophistication in operator procedural support.

7. ACKNOWLEDGEMENTS

The GRADIENT Project (P857) commenced in October 1985 and has the following consortium: Axion A/S, Birkerod, Denmark (prime contractor); Asea Brown Boveri, Central Research Laboratory, Heidelberg, West Germany; University of Kassel, Laboratory for Man-Machine Systems, Kassel, West Germany; University of Leuven, Chemical Engineering Department, Leuven, Belgium; University of Strathclyde, Scottish HCI Centre, Glasgow, United Kingdom. The contribution of all partners to this work is gratefully acknowledged.

8. REFERENCES

Alty, J. L. & Weir, G. R. S. (1987). Dialogue for dynamic systems. In *ESPRIT '87: Achievements and impact*, pp. 819-825. Amsterdam: North-Holland.

Bainbridge, L. (1987). (1987). Ironies of automation. In J. Rasmussen, K. Duncan & J. Leplat (Eds.), *New technology and human error*, pp. 271-283. London: Wiley.

Degani, A. & Wiener, E. L. (1990). *Human factors of flight-deck checklists: The normal checklist* (NASA CR-177549). Washington, D. C.: NASA.

De Keyser, V. (1986). Technical assistance to the operator in case of incident: Some lines of thought. In E. Hollnagel, G. Mancini & D. D. Woods (Eds.), *Intelligentr decision support in process environments*, pp. 229-253. Heidelberg: Springer Verlag.

Hollnagel, E. (1990). The phenotype of erroneous actions: Implications for HCI design. In G. R. S. Weir & J. L. Alty (Eds.), *Human-computer interaction and complex systems*. London: Academic Press.

Hollnagel, E., Embrey, D. & Cain, D. *Computer based aids for operator support in nuclear power plants* (IAEA-TECDOC-549). Vienna: IAEA.

Rouse, S. H. & Rouse, W. B. (1980). Computer based manuals for procedural information. *IEEE Transactions on System, Man, and Cybernetics, 10*(8), 506-510.

Woods, D. D. (1990). The cognitive engineering problem of representations. In G. R. S. Weir & J. L. Alty (Eds.), *Human-computer interaction and complex systems*. London: Academic Press.

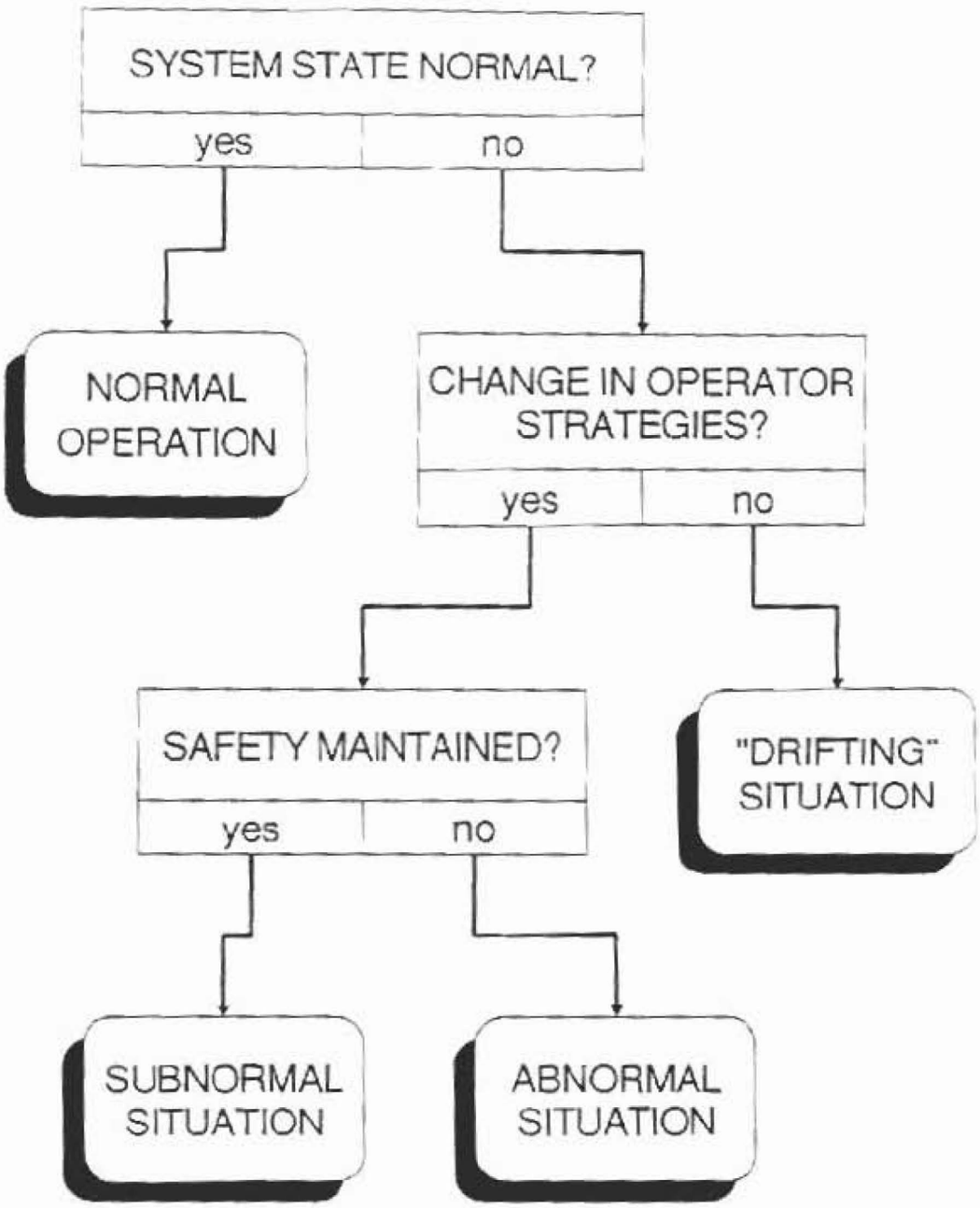

Figure 1: Four Typical Operating Situations

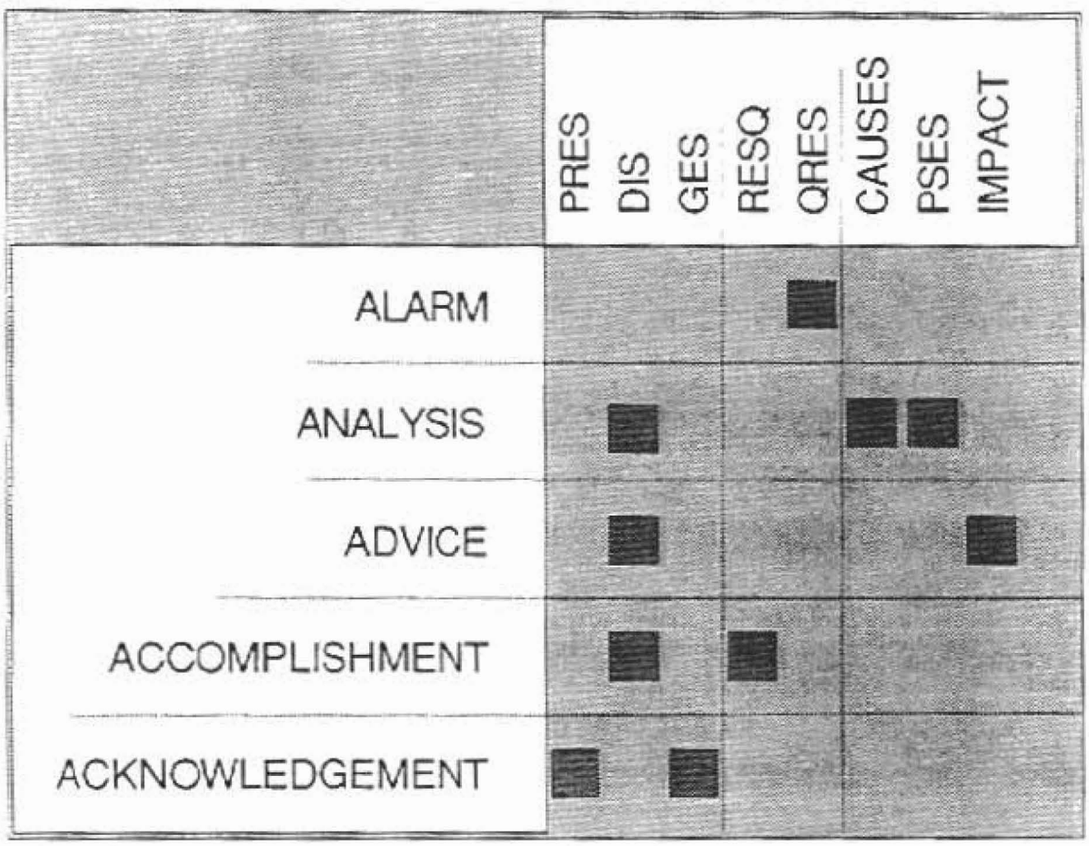

Figure 2: Varieties Of GRADIENT Support

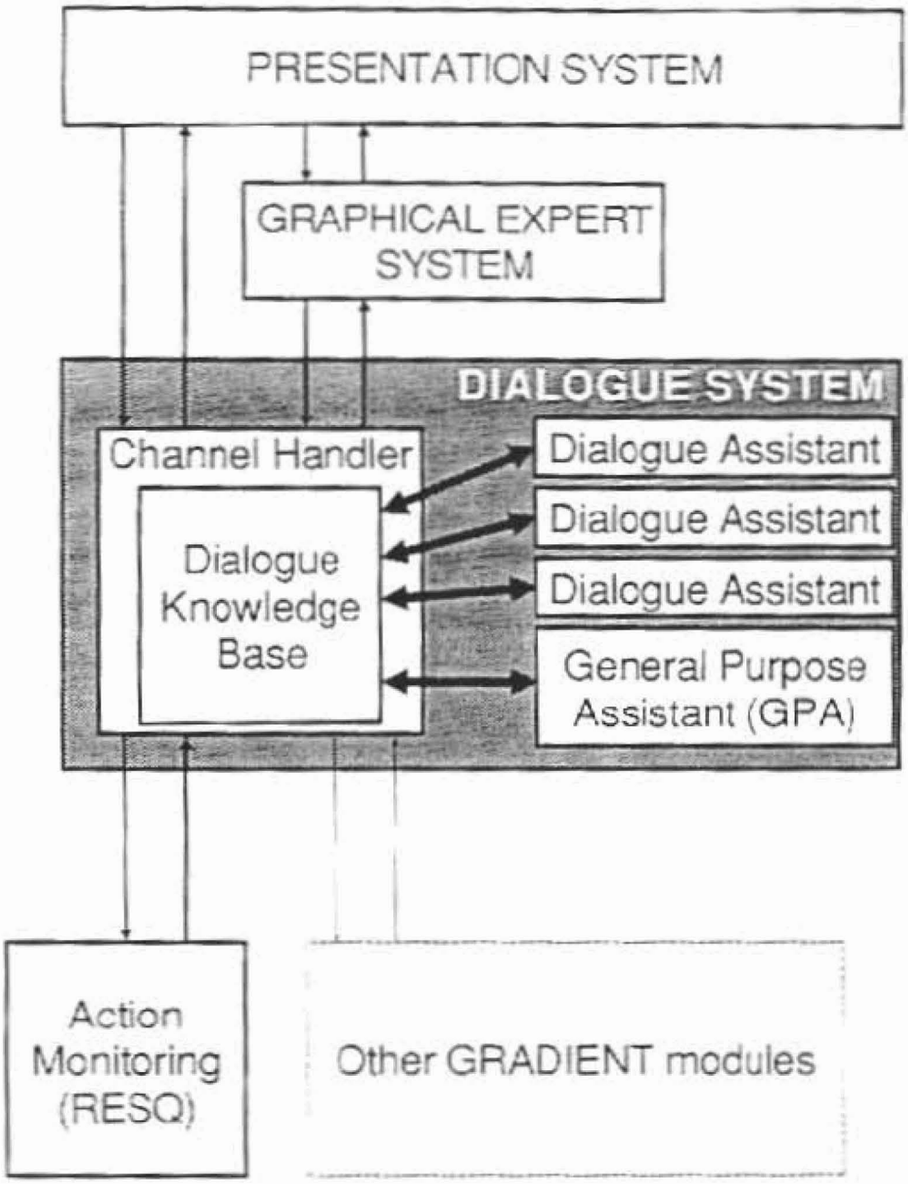

Figure 3: The Architecture of DIS within GRADIENT

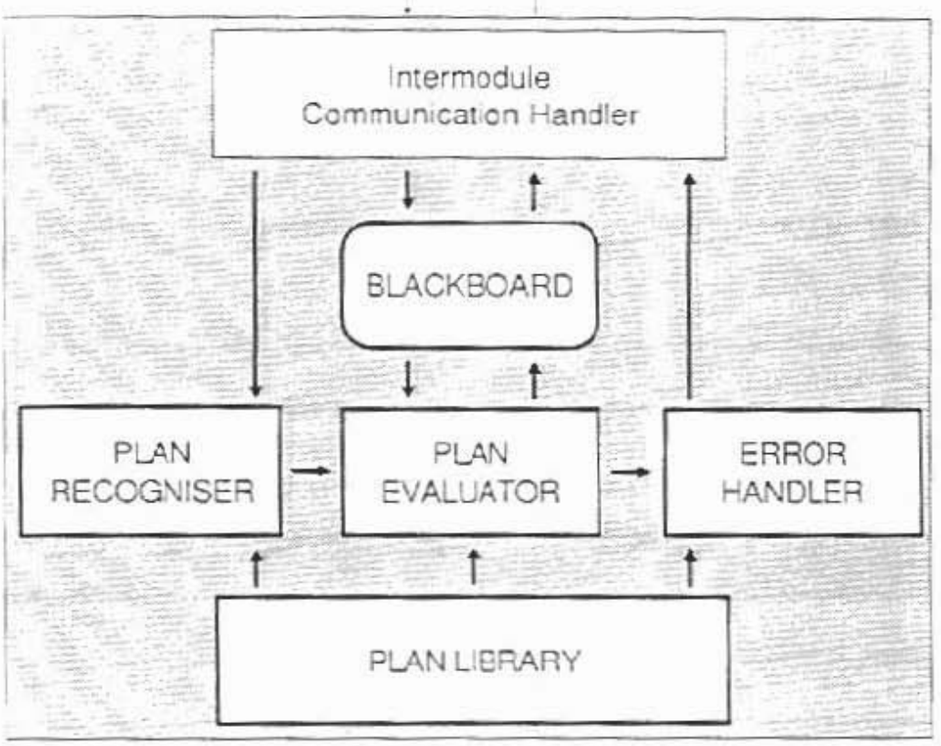

Figure 4: The Architecture of RESQ